PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-105470
(43)Date of publication of application : 24.04.1998

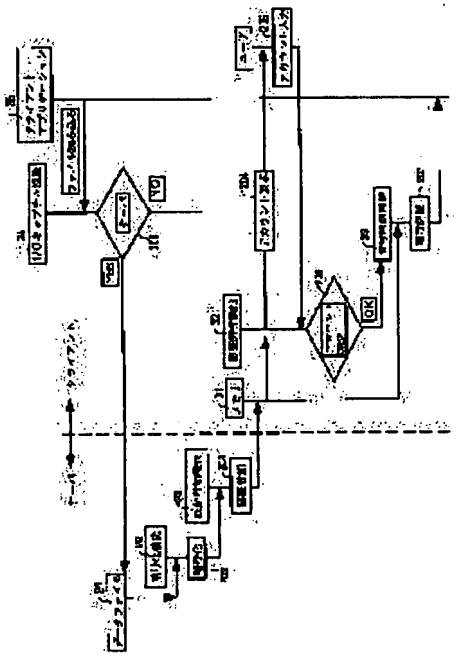
(51)Int.Cl. G06F 12/14
G06F 12/00

(21)Application number : 08-257186
(22)Date of filing : 27.09.1996

(71)Applicant : HITACHI SOFTWARE ENG CO LTD
(72)Inventor : SAITO KAZUMASA

(54) METHOD FOR AUTHENTICATING FILE ACCESS

(57)Abstract:
PROBLEM TO BE SOLVED: To disenable accessing to a common file unless a user is the normal one authenticated by means of a server by permitting a client side to succeed an authentication for an access request to the common file which is managed by means of the server even in an off-line state.
SOLUTION: When the requested common file is transferred to a client for the access request to the comman file from the client to the server, the common file is enciphered 202 and transferred with acount information managed on the server. When access to the common file is permitted in the client, an authentication processing 32 consisting of at least a user name and a password is executed, the enciphered common file is decoded only when the user is authenticated to be the normal one 207 so as to make access possible. At the time of access completion, the decoded common file is enciphered so as to be preserved in the local storage medium of the client and the authentication processing is also executed at the time of requesting access to the preserved common file.



LEGAL STATUS

[Date of request for examination] 07.04.1999
[Date of sending the examiner's decision of rejection] 14.07.2003
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－105470

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]		識別記号	FI		
G06F	12/14	320	G06F	12/14	320B
					320C
	12/00	545		12/00	545F

審査請求　未請求　請求項の数1　OL　（全７頁）

(21)出願番号　特願平8－257186

(22)出願日　平成８年(1996)９月27日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　齊藤　和政
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

(54)【発明の名称】　ファイルアクセス認証方法

(57)【要約】

【課題】　サーバが管理している共有ファイルへのアクセス要求に対する認証をオフラインの状態においてもクライアント側に継承し、サーバが認証する正規のユーザでなければ共有ファイルに対するアクセスを不可能にする。

【解決手段】　クライアントからサーバに対する共有ファイルへのアクセス要求に対し、要求された共有ファイルをクライアントに転送するに際し、当該共有ファイルを暗号化し、かつサーバ上で管理するアカウント情報を添付して転送し、クライアントにおいては当該共有ファイルに対するアクセスを許可する際に、少なくともユーザ名およびパスワードから成る認証処理を実施し、正規のユーザであると認証されたときのみ暗号化された共有ファイルを復号してアクセス可能とし、アクセス終了時には復号した共有ファイルを暗号化してクライアントのローカル記憶媒体に保存し、その保存された共有ファイルに対するアクセス要求時にも認証処理を実施する。

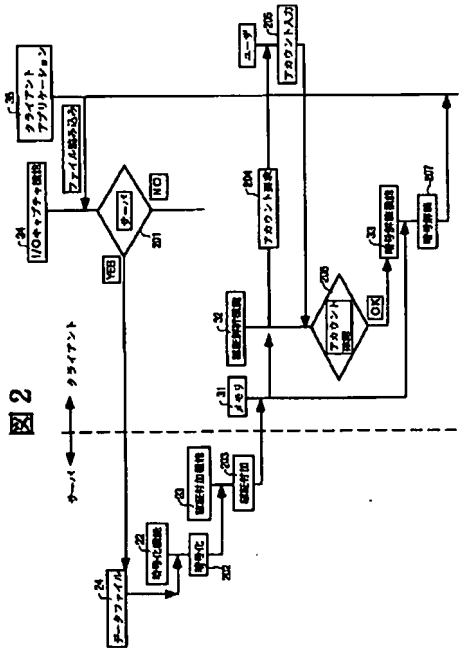


図２

1

【特許請求の範囲】

【請求項１】　ファイル共有型のサーバ・クライアント型ネットワークシステムにおけるファイルアクセス認証方法であって、

クライアントからサーバに対する共有ファイルへのアクセス要求に対し、要求された共有ファイルをクライアントに転送するに際し、当該共有ファイルを暗号化し、かつサーバ上で管理するアカウント情報を添付して転送し、クライアントにおいては当該共有ファイルに対するアクセスを許可する際に、少なくともユーザ名およびパスワードから成る認証処理を実施し、正規のユーザであると認証されたときのみ暗号化された共有ファイルを復号してアクセス可能とし、アクセス終了時には復号した共有ファイルを暗号化してクライアントのローカル記憶媒体に保存し、その保存された共有ファイルに対するアクセス要求時にも認証処理を実施することを特徴とするファイルアクセス認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ファイル共有型のサーバ・クライアント型ネットワークシステムにおけるファイルアクセス認証方法に係り、特に、サーバが管理している共有ファイルをクライアント内のメモリにコピーしてオフラインで携帯して利用するモバイルコンピューティングと呼ばれる利用形態の場合にも、サーバ上で認証を与えたユーザのみが共有ファイルにアクセスすることが可能になるようにしたファイルアクセス認証方法に関するものである。

【０００２】

【従来の技術】従来、ＬＡＮ等を前提としたファイル共有型のサーバ・クライアント型ネットワークシステムにおいては、クライアントからサーバが管理している共有ファイルへのアクセス要求があった際に、そのアクセス要求に対する認証は、クライアントがサーバにログイン等の手続きを行う際に使用するアカウント情報に関して、サーバの認証機能がアクセス可否を判断するという方法で実施されている。

【０００３】

【発明が解決しようとする課題】しかし、上記従来の認証方法にあっては、クライアントがサーバ上の共有ファイルにアクセスする場合、サーバ側ではクライアントがログインしている事を前提としているため、クライアントがサーバの認証を受けて、サーバ上の共有ファイルをクライアント上の記憶媒体にコピーした後、オフライン状態とし、コピーされた共有ファイルにアクセスしようとする際は、サーバの認証を受ける必要がなくなる。このため、一旦、クライアント上の記憶媒体にコピーされた共有ファイルはユーザが誰であってもアクセス可能となってしまうという問題点が発生する。

【０００４】本発明は、上述のような各々の問題点を解決するためになされたものであり、その目的は、サーバが管理している共有ファイルへのアクセス要求に対する認証を、オフラインの状態においてもクライアント側に継承し、共有ファイルへのアクセスを完全にサーバでコントロールし、サーバが認証する正規のユーザでなければ共有ファイルに対するアクセスを不可能とし、機密性の高いデータ等が不正に使用されないようにすることができるファイルアクセス認証方法を提供することにある。

2

【０００５】

【課題を解決するための手段】上記の目的を達成するために、本発明のファイルアクセス認証方法は、クライアントからサーバに対する共有ファイルへのアクセス要求に対し、要求された共有ファイルをクライアントに転送するに際し、当該共有ファイルを暗号化し、かつサーバ上で管理するアカウント情報を添付して転送し、クライアントにおいては当該共有ファイルに対するアクセスを許可する際に、少なくともユーザ名およびパスワードから成る認証処理を実施し、正規のユーザであると認証されたときのみ暗号化された共有ファイルを復号してアクセス可能とし、アクセス終了時には復号した共有ファイルを暗号化してクライアントのローカル記憶媒体に保存し、その保存された共有ファイルに対するアクセス要求時にも認証処理を実施することを特徴とする。

【０００６】

【発明の実施の形態】以下、本発明の実施形態を図面を用いて詳細に説明する。

【０００７】図１は、ＬＡＮを前提としたファイル共用型のサーバ・クライアントシステムの主要部の実施形態を示すブロック図である。

【０００８】図１において、１はサーバマシン２とクライアントマシン３間を結ぶネットワーク、例えばＬＡＮである。２は共用ファイルを管理するサーバマシン、３はクライアントマシンであり、サーバマシン２とクライアントマシン３はネットワーク１を介してファイル共用型のシステムを実現している。

【０００９】２１はサーバマシン２上の認証機能、２２はサーバマシン２が管理する共有ファイルへのアクセス要求がクライアントマシン３からあった場合に、要求された共有ファイルに暗号化を施す暗号化機能、２３は共有ファイルへのアクセス要求があった場合に、同ファイルにアクセス権限のあるアカウントを、アカウントとアクセス権限一覧の形式でサーバマシン２の認証機能２１から受け取り、要求されたファイルに添付する認証付加機能である。これらの認証機能２１，暗号化機能２２，認証付加機能２３は、それぞれ認証処理プログラム，暗号化プログラム，認証付加処理プログラムというプログラムによって実現されている。

【００１０】２４はサーバマシン２が管理し、複数のクライアントマシン３が共用しているデータファイル（共

用ファイル）である。

【００１１】一方、３１はクライアントマシン３が管理するローカルのメモリであり、サーバマシン２から受け取ったファイルは、一旦、このローカルのメモリ３１に格納される。

【００１２】３２はサーバマシン２から受け取り、かつメモリ３１に格納されたファイルに対しクライアントマシン３のアプリケーションプログラム３５がアクセスする際、アクセス権限のチェックを行う認証解析機能であり、この認証解析機能３２はメモリ３１上の受信ファイルにアプリケーションプログラム３５がアクセス（読み込み、書き込み）を行おうとする際、アプリケーションプログラム３５のユーザに対し、アカウント情報とパスワードの入力を要求する。さらに、認証解析機能３２は、入力されたアカウント情報と、メモリ３１内の受信ファイルに添付されたアカウント情報およびアクセス権一覧を突き合わせ、同アカウント情報が受信ファイルにアクセス権限を持つかどうかを検証する。アクセス権を持つ場合に限り、暗号化解読機能３３と連携し、アプリケーションプログラム３５のユーザにデータアクセスを許可する。

【００１３】３３は暗号化解析機能であり、認証解析機能３２から呼び出され、認証解析機能がアクセスを許可したメモリ３１内の受信ファイルに対し、サーバマシン２の暗号化機能２２によって受信ファイルに施された暗号化を外し、復号する。

【００１４】３４はアプリケーションプログラム３５からの受信ファイルに対するアクセスをキャプチャし、認証と暗号化を施された受信ファイルに対するアクセスを許可するか否かを判別するＩ／Ｏキャプチャ機能、３６は復号されてメモリ３１内に格納された受信ファイルをアプリケーションプログラム３５からのアクセス終了時に再度暗号化して格納するための暗号化機能である。

【００１５】これらの認証解析機能３２，暗号解読機能３３，Ｉ／Ｏキャプチャ機能３４，暗号化機能３６は、それぞれ認証解析処理プログラム，暗号解読処理プログラム，Ｉ／Ｏキャプチャプログラム，暗号化処理プログラムといったプログラムで実現されている。

【００１６】図２は、クライアントマシン側のアプリケーションプログラム３５によるデータファイル２４の読み込みのシーケンス図である。

【００１７】アプリケーションプログラム３５から発行されたデータ読み込み命令（ファイルアクセス要求）は、一旦、Ｉ／Ｏキャプチャ機能３４によって判定され、サーバマシン２のデータファイル２４に対するアクセスであるか否かが確認される（ステップ２０１）。そして、データファイル２４に対するアクセスであると確認された時のみ、サーバマシン２にネットワーク１を通じて転送される。

【００１８】これに対しサーバマシン２は、クライアントマシン３から要求されたファイルをデータファイル２４内から検索し、そのファイルに対し、暗号化機能２２によって暗号化を施し（ステップ２０２）、さらにその暗号化したファイルに対し認証付加機能２３によってアカウント情報を添付し（ステップ２０３）、クライアントマシン３にネットワーク１経由で転送する。

【００１９】クライアントマシン３は、受信したファイルをメモリ３１に一旦格納する。次に、クライアントマシン３の認証解析機能３２は、メモリ３１にファイルが格納されたならば、ファイルアクセス要求をアプリケーションプログラム３５から発行したユーザに対してアカウント情報の入力を要求し（ステップ２０４）、ユーザからアカウント情報が入力されたならば（ステップ２０５）、ユーザから入力されたアカウント情報でメモリ３１内の受信ファイルにアクセスが可能かどうかを当該受信ファイルに添付された認証情報と突き合わせ（ステップ２０６）、アクセス可能であれば暗号化された受信ファイルを暗号解読機能３３によって復号し（ステップ２０７）、Ｉ／Ｏキャプチャ機能３４を介してアプリケーションプログラム３５に渡す。

【００２０】ユーザがアプリケーションプログラム３５からの復号されたファイルへのアクセスを終了した場合、暗号化機能３６は、復号されたファイルのデータをサーバマシン２の暗号化処理と同様にして再度暗号化し、メモリ３１内に格納する。

【００２１】要するに、クライアントマシン３のメモリ３１またはカードメモリ等のメモリに復号したファイルデータは、再び、同様の認証処理を受けた後にアクセス可能とするために、再度暗号化して格納される。

【００２２】図３は、クライアントマシン２に設けたデータファイル３７に、サーバマシン２から受信したファイルのコピーを保持させ、オフラインで作業するモバイルコンピューティングの際のシーケンスを示す図であり、クライアントマシン３のデータファイル（クライアント記憶装置）３７にコピーされたファイルは、サーバマシン２において認証情報が添付され、かつ暗号化されたファイルとなっている。

【００２３】このデータファイル３７をクライアントマシン３からユーザがアクセスする際にも、図２と同様のシーケンスで認証処理が実施され、アクセス可能なアカウント情報およびパスワードが入力された時のみ暗号化が解かれる。

【００２４】よって、オフライン状態であっても、オンライン状態と同様の認証処理を経てアクセスが許可される。これによって、クライアントマシン３内にコピーしたファイルを保存しておいたとしても、サーバマシン２が認めた正規のユーザ以外はアクセスすることが不可能になり、機密性の高いデータが正規のユーザ以外に漏れてしまうのを防止することが可能になる。

【００２５】

5

【発明の効果】以上説明したように、本発明においては、クライアントからサーバに対する共有ファイルへのアクセス要求に対し、要求された共有ファイルをクライアントに転送するに際し、当該共有ファイルを暗号化し、かつサーバ上で管理するアカウント情報を添付して転送し、クライアントにおいては当該共有ファイルに対するアクセスを許可する際に、少なくともユーザ名およびパスワードから成る認証処理を実施し、正規のユーザであると認証されたときのみ暗号化された共有ファイルを復号してアクセス可能とし、アクセス終了時には復号した共有ファイルを暗号化してクライアントのローカル記憶媒体に保存し、その保存された共有ファイルに対するアクセス要求時にも認証処理を実施するようにしたため、サーバが管理している共有ファイルへのアクセス要求に対する認証が、オフラインの状態においてもクライアント側に継承され、サーバが認証する正規のユーザでなければ共有ファイルに対するアクセスが不可能になる。

【００２６】これによって、クライアントとサーバとがオフラインの状態であっても、クライアント内にコピーしておいたデータをアクセスすることができなくなり、機密性の高いデータ等が不正に使用されないようにすることができる。

6

【図面の簡単な説明】

【図１】本発明を適用したファイル共用型サーバ・クライアントシステムの要部の実施形態を示すブロック図である。

【図２】図１のクライアント側アプリケーションプログラムによる共有ファイルの読み込み時のシーケンス図である。

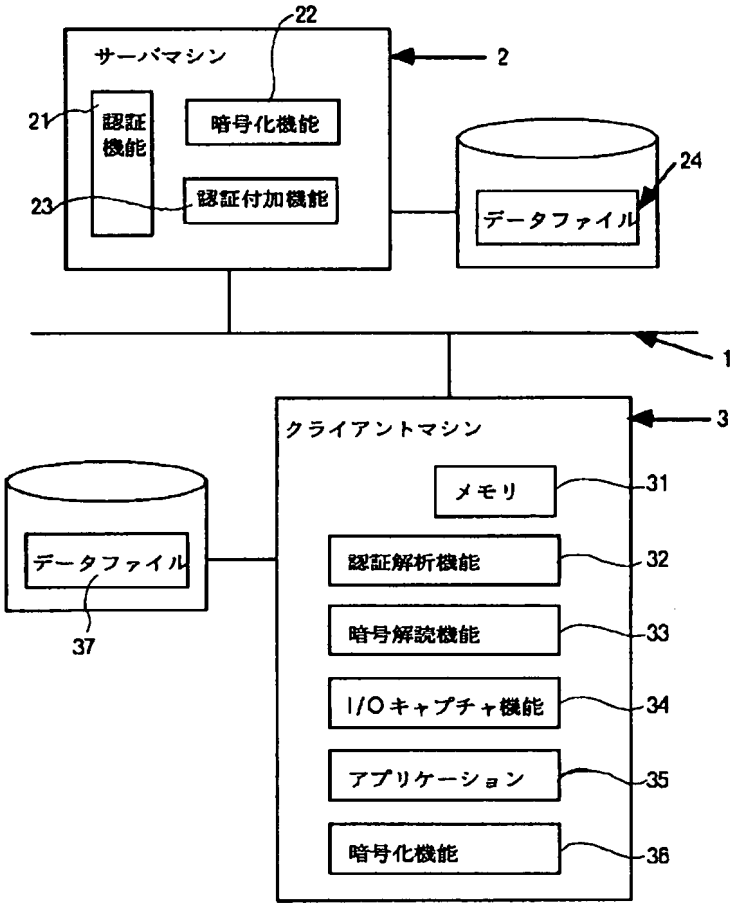
【図３】クライアント側に共有ファイルのコピーを保持し、オフラインで作業するモバイルコンピューティングの際のシーケンス図である。

【符号の説明】

１…ネットワーク、２…サーバマシン、３…クライアントマシン、２１…認証機能、２２…暗号化機能、２３…認証付加機能、２４…データファイル、３１…ローカルのメモリ、３２…認証解析機能、３３…暗号化解析機能、３４…Ｉ／Ｏキャプチャ機能、３５…アプリケーションプログラム、３６…暗号化機能。

【図１】

図１


22
サーバマシン
2
21
認証機能
暗号化機能
23
認証付加機能
24
データファイル
1
3
クライアントマシン
メモリ
31
データファイル
認証解析機能
32
暗号解読機能
33
I/Oキャプチャ機能
34
アプリケーション
35
暗号化機能
36
37

【図２】

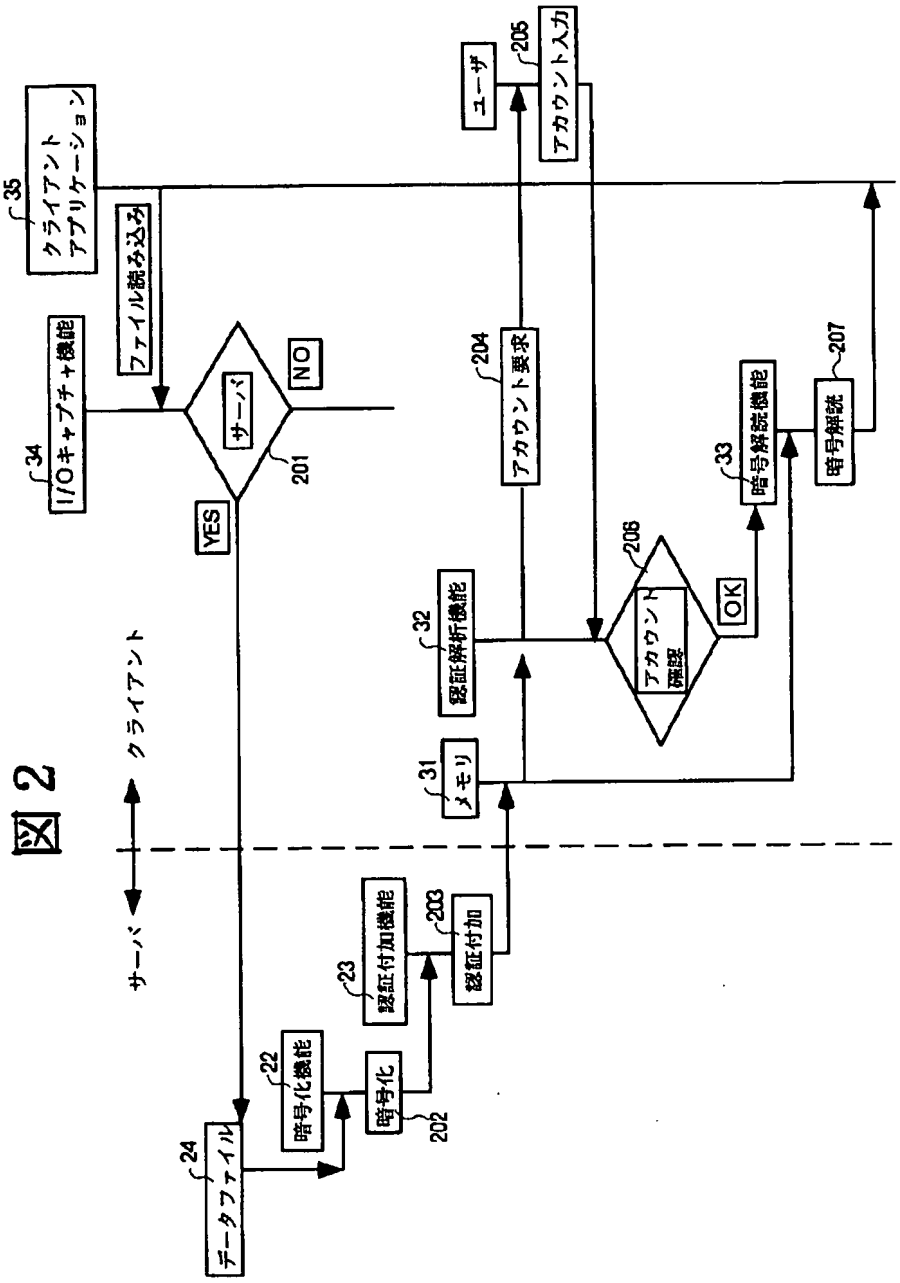


図２
サーバ
クライアント
35 クライアントアプリケーション
34 I/Oキャプチャ機能
ファイル読み込み
サーバ
201
NO
YES
24 データファイル
22 暗号化機能
暗号化
202
23 認証付加機能
203 認証付加
31 メモリ
32 認証解析機能
204 アカウント要求
ユーザ
205 アカウント入力
206 アカウント確認
OK
33 暗号解読機能
207 暗号解読

【図3】

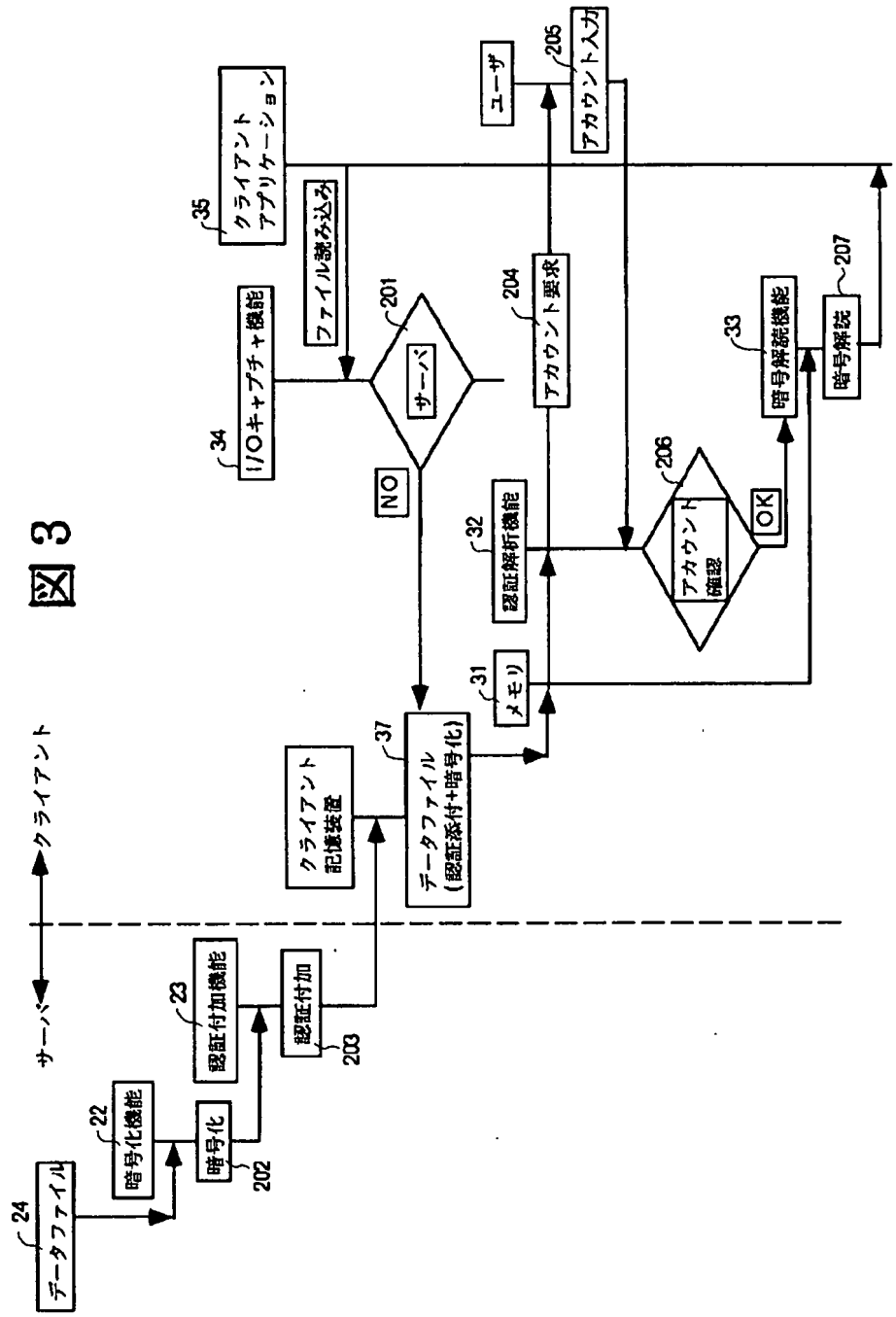


図3
サーバ
クライアント
24 データファイル
22 暗号化機能
暗号化
202
23 認証付加機能
認証付加
203
クライアント記憶装置
37 データファイル（認証添付+暗号化）
31 メモリ
32 認証解析機能
NO
201 サーバ
34 I/Oキャプチャ機能
ファイル読み込み
35 クライアントアプリケーション
ユーザ
205 アカウント入力
204 アカウント要求
206 アカウント確認
OK
33 暗号解読機能
暗号解読
207

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is the file access authentication approach in the server client mold network system of a file-sharing mold. As opposed to the access request from a client to the shared file to a server Face transmitting the demanded shared file to a client, and the shared file concerned is enciphered. And in case the account information managed on a server is attached and transmitted and access to the shared file concerned is permitted in a client Carry out authentication processing which consists of a user name and a password at least, decode the shared file enciphered only when attested with his being the user of normal, and it is supposed that it is accessible. The file access authentication approach characterized by enciphering the decoded shared file at the time of access termination, saving at the local storage of a client, and carrying out authentication processing also at the time of the access request to the saved shared file.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the file access authentication approach in the server client mold network system of a file-sharing mold, copies the shared file which the server has managed especially to the memory in a client, and relates to the file access authentication approach of having made it enable only the user who gave authentication on the server also in the case of the use gestalt called mobile computing carried and used off-line to access a shared file.
[0002]
[Description of the Prior Art] When there is an access request to the shared file which the server has managed from the client conventionally in the server client mold network system of the file-sharing mold on condition of LAN etc., authentication over the access request is carried out by the approach the authentication function of a server judges access propriety, about the account information used in case a client takes the necessary procedure for a log in etc. to a server.
[0003]
[Problem(s) to be Solved by the Invention] In case it is going to consider as an offline state and is going to access the copied shared file after a client copies the shared file on a server to the storage on a client in response to authentication of a server, it becomes unnecessary however, to receive authentication of a server by the server side, since it is premised on the client logging in when a client accesses the shared file on a server, if it is in the above-mentioned conventional authentication approach. For this reason, even if a user is whom, the trouble of being accessible once generates the shared file copied to the storage on a client.
[0004] It is made in order that this invention may solve each above troubles. The purpose The authentication over the access request to the shared file which the server has managed Also in an off-line condition, succeed to a client side, and access to a shared file is completely controlled by the server. If it is not the user of the normal which a server attests, access to a shared file will be made impossible, and it is in offering the file access authentication approach that it can avoid using the high data of confidentiality etc. unjustly.
[0005]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the file access authentication approach of this invention As opposed to the access request from a client to the shared file to a server Face transmitting the demanded shared file to a client, and the shared file concerned is enciphered. And in case the account information managed on a server is attached and transmitted and access to the shared file concerned is permitted in a client Carry out authentication processing which consists of a user name and a password at least, decode the shared file enciphered only when attested with his being the user of normal, and it is supposed that it is accessible. The decoded shared file is enciphered at the time of access termination, and it saves at the local storage of a client, and is characterized by carrying out authentication processing also at the time of the access request to the saved shared file.

[0006]
[Embodiment of the Invention] Hereafter, the operation gestalt of this invention is explained to a detail using a drawing.
[0007] Drawing 1 is the block diagram showing the operation gestalt of the principal part of the client/server architecture of the file common mold on condition of LAN.
[0008] In drawing 1 , 1 is the network to which between a server machine 2 and a client machine 3 is connected, for example, LAN. The server machine with which 2 manages a shared file, and 3 are client machines, and the server machine 2 and the client machine 3 have realized the system of a file common mold through a network 1.
[0009] The encryption function which enciphers to the demanded shared file when there is an access request to the shared file to which the authentication function on a server machine 2 manages 21, and a server machine 2 manages 22 from a client machine 3, and 23 are the authentication addition function which attaches to the reception from the authentication function 21 of a server machine 2, and the demanded file in the form of account and an access permission list of the account which has an access permission in this file, when there is an access request to a shared file. These authentication functions 21, the encryption function 22, and the authentication addition function 23 are realized by the program of an authentication processing program, an encryption program, and an authentication attached-processing program, respectively.
[0010] 24 is a data file (shared file) which a server machine 2 manages and two or more client machines 3 are sharing.
[0011] On the other hand, 31 is local memory which a client machine 3 manages, and the file received from the server machine 2 is once stored in this local memory 31.
[0012] 32 is an authentication analysis feature which checks an access permission in case the application program 35 of a client machine 3 accesses from a server machine 2 to the file stored in reception and memory 31, and this authentication analysis feature 32 requires the input of account information and a password of the user of an application program 35, in case an application program 35 tends to access the reception file on memory 31 (reading writing). Furthermore, the authentication analysis feature 32 compares the inputted account information, the account information attached to the reception file in memory 31, and an access privilege list, and verifies whether this account information has an access permission in a reception file. It restricts, when it has an access privilege, and it cooperates with the encryption decode function 33, and a data access is permitted to the user of an application program 35.
[0013] 33 is an encryption analysis feature, is called from the authentication analysis feature 32, and removes and decodes the encryption given to the reception file by the encryption function 22 of a server machine 2 to the reception file in the memory 31 which the authentication analysis feature permitted access.
[0014] It is an encryption function for enciphering again and storing the reception file which 34 carried out the capture of the access to the reception file from an application program 35, and the I/O capture function which distinguishes whether authentication and access to the reception file to which encryption was given are permitted, and 36 were decoded, and was stored in memory 31 at the time of the access termination from an application program 35.
[0015] These authentication analysis features 32, the decryption function 33, the I/O capture function 34, and the encryption function 36 are realized by the authentication analysis processing program, the decryption processing program, the I/O capture program, and the program of an encryption processing program, respectively.
[0016] Drawing 2 is the sequence diagram of reading of the data file 24 by the application program 35 by the side of a client machine.
[0017] The data reading instruction (file access demand) published from the application program 35 is once judged by the I/O capture function 34, and it is checked whether it is access to the data file 24 of a server machine 2 (step 201). And only when it is checked that it is access to a data file 24, it is transmitted to a server machine 2 through a network 1.
[0018] On the other hand, the file demanded from the client machine 3 is searched out of a data file 24,

and to the file, a server machine 2 enciphers by the encryption function 22 (step 202), to the enciphered file, it attaches account information (step 203) and transmits it to a client machine 3 by network 1 course by the authentication addition function 23 further.
[0019] A client machine 3 once stores the file which received in memory 31. Next, the authentication analysis feature 32 of a client machine 3 If a file is stored in memory 31, the input of account information will be required of the user who published the file access demand from the application program 35 (step 204). If account information is inputted from a user (step 205) It compares with the authentication information attached [whether the reception file in memory 31 can be accessed by the account information inputted by the user, and] to the reception file concerned (step 206). If accessible, the enciphered reception file will be decoded by the decryption function 33 (step 207), and an application program 35 will be passed through the I/O capture function 34.
[0020] When a user ends access to the file decoded from the application program 35, the encryption function 36 enciphers the data of the decoded file again like encryption processing of a server machine 2, and stores them in memory 31.
[0021] In short, after receiving the same authentication processing again, since it is accessible, it enciphers again and the file data decoded in memory, such as the memory 31 of a client machine 3 or card memory, is stored.
[0022] The file which is drawing showing the sequence in the case of mobile computing which is made to hold the copy of the file which received from the server machine 2 to the data file 37 which prepared drawing 3 in the client machine 2, and works off-line to it, and was copied at the data file (client store) 37 of a client machine 3 is the file as which authentication information was attached and it was enciphered in the server machine 2.
[0023] Also in case a user accesses this data file 37 from a client machine 3, authentication processing is carried out by the same sequence as drawing 2 , and encryption is solved only when accessible account information and an accessible password are entered.
[0024] Therefore, even if it is an offline state, access is permitted through the same authentication processing as an on-line state. Even if it saved the file copied in the client machine 3 by this, accessing becomes impossible except the user of normal whom the server machine 2 accepted, and it becomes possible to prevent that the high data of confidentiality leak in addition to the user of normal.
[0025]
[Effect of the Invention] As opposed to the access request to a shared file [as opposed to / in / as explained above / this invention / the server from a client] Face transmitting the demanded shared file to a client, and the shared file concerned is enciphered. And in case the account information managed on a server is attached and transmitted and access to the shared file concerned is permitted in a client Carry out authentication processing which consists of a user name and a password at least, decode the shared file enciphered only when attested with his being the user of normal, and it is supposed that it is accessible. In order to encipher the decoded shared file at the time of access termination, to save at the local storage of a client and to carry out authentication processing also at the time of the access request to the saved shared file, The authentication over the access request to the shared file which the server has managed is inherited by the client side also in an off-line condition, and if it is not the user of the normal which a server attests, access to a shared file will become impossible.
[0026] It becomes impossible to access the data copied in the client, and this can be prevented from using the high data of confidentiality etc. unjustly, even if a client and a server are in an off-line condition.

[Translation done.]

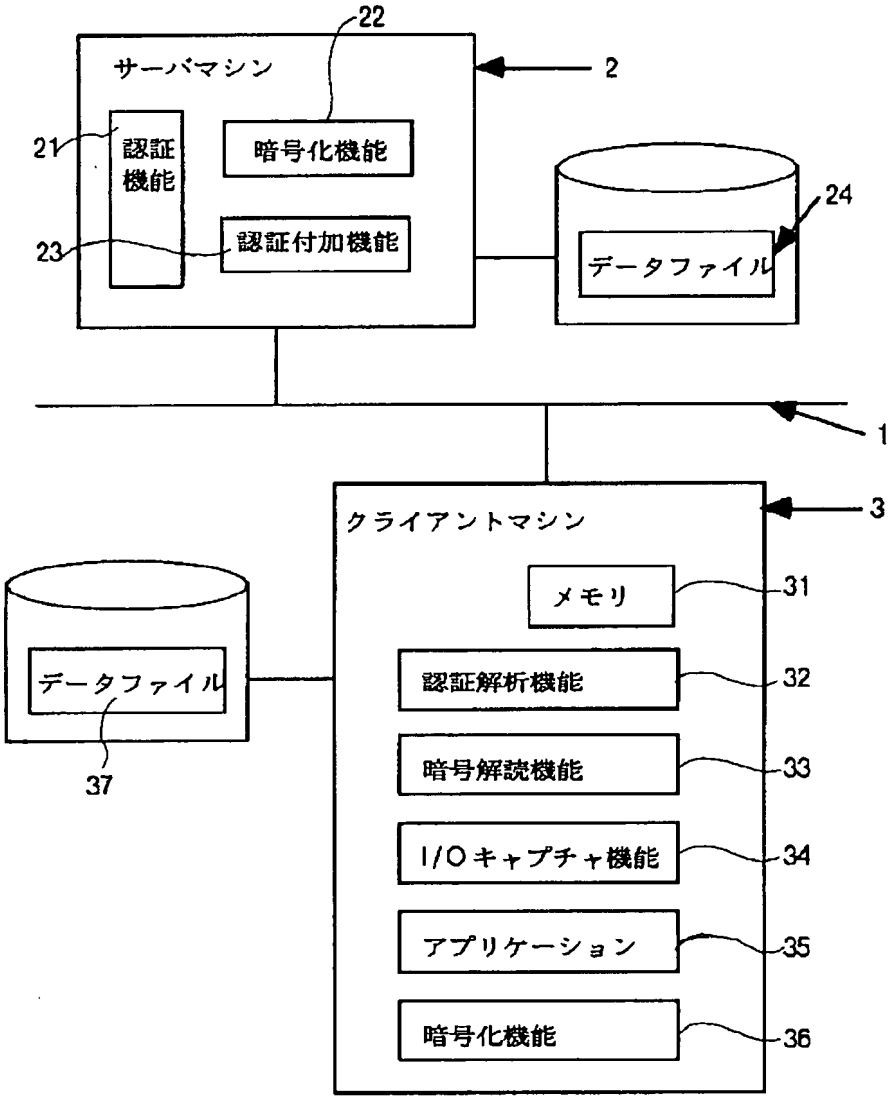
* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]

図 1



[Drawing 2]

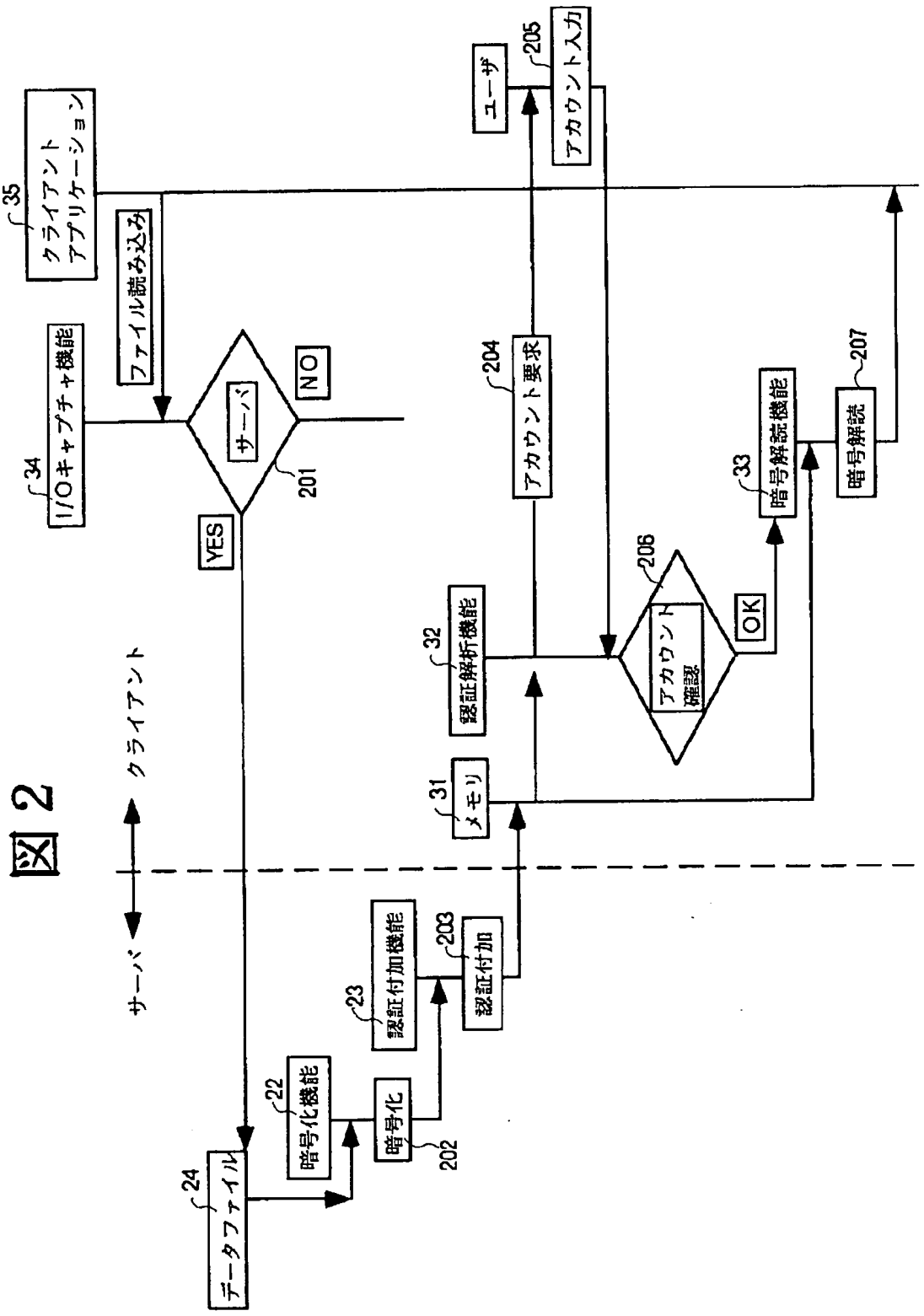
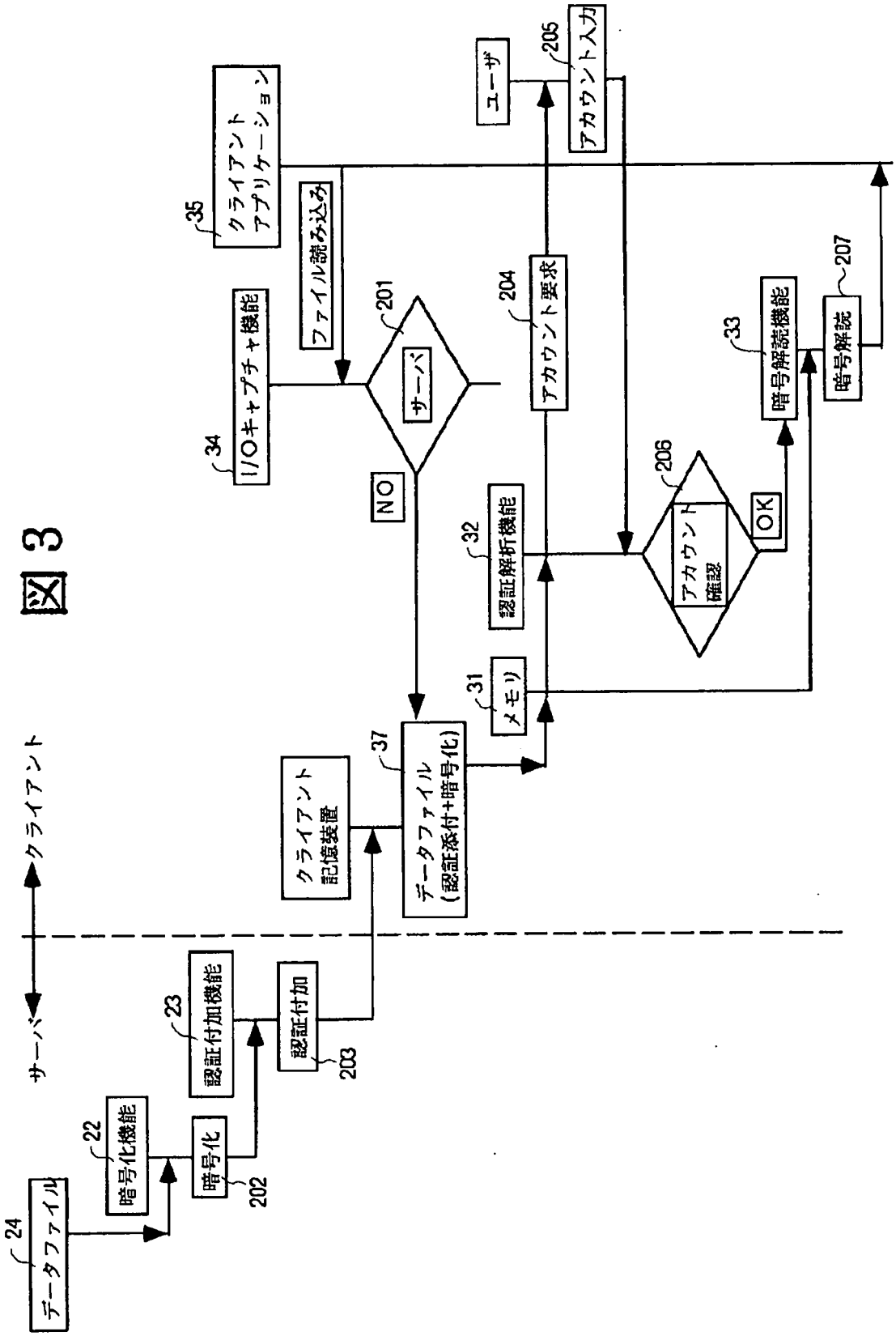

クライアント
サーバ
35 クライアントアプリケーション
ファイル読み込み
34 I/Oキャプチャ機能
サーバ
201
NO
YES
ユーザ
205 アカウント入力
204 アカウント要求
206 アカウント確認
OK
33 暗号解読機能
207 暗号解読
32 認証解析機能
31 メモリ
23 認証付加機能
203 認証付加
22 暗号化機能
暗号化
202
24 データファイル

図2

[Drawing 3]

図3



[Translation done.]